AMENDMENTS TO THE SPECIFICATION:

Please amend the Examiner's Amended Specification version which accompanied the Notice of Allowability as follows:

--SUMMARY ~~OF THE INVENTION:~~

The present invention provides a method for encrypting data according to an asymmetrical method, based on a factorization problem, having a public key and a private key; the public key being the interation number L as well as the composite number n, n preferably being the product of a plurality of large prime numbers; the private key is made up of the factorization of n; the message $m = (m_1, m_2)$ to be encrypted is made up of at least components m_1 and m_2; an encryption function f(x) is iterated a total of L times, with $c=(c_1, c_2)= f^L(m)$; $f(m)=(f_1(m), f_2(m))$ being applicable, and $f_1=(m_1 op_1 m_2) \bmod n$ as well as $f_2=(m_1, op_2 m_2) \bmod n$; op_1 being, for example, an addition and op_2 being, for example, a multiplication. The encryption function f(x) is selected in such a way that the encryption iteration can be reversed by the L-fold solution of a quadratic equation modulo n, it thus being possible to retrieve the original message from the encrypted information $c=(c_1, c_2)$. In an embodiment, a multivaluedness of the quadratic equation is eliminated by additional bits of a_i and b_i. In an embodiment, the multivaluedness of the quadratic equation is eliminated by calculating a parity and a Jacobi symbol which, for example, in the case of prime numbers of form 3 mod ~~rood~~ 4, can be communicated by 2 bits per iteration step. In an embodiment, general iterations $f1=(k1 \bullet m1+k2 \bullet m2) \bmod n$ as well as $f2=(k3 \bullet m1 \bullet m2) \bmod n$ are used, constants being part of the public key. In an embodiment, the composite number n as public key contains more than two factors. In an embodiment, the message is now made up of an N-tuple $m=(m_1 \ldots m_{N\#})$, the formula for the Lth iteration step using dependencies of N values in each iteration step. In an embodiment, the multivaluedness is resolved by additional bits that are derived from the values obtained in each iteration. In an embodiment, the multivaluedness is resolved by redundancy in the transmitted data.

The present invention provides a method for generating a signature, wherein a signature is generated by interchanging the encryption and decryption steps from one or more of the method embodiments described herein. The present invention provides a software for a computer which implements one or more of the method embodiments described herein. That is, the software is ~~being~~ instructions configured to be executed by the computer; ~~,~~ the

instructions which, when executed by the computer, cause the performance of one or more of the method embodiments described herein. ~~the~~ The present invention provides for a data carrier for a computer, characterized by the storage of software for the computer which implements one or more of the method embodiments described herein.

DETAILED ~~DETAIL~~ DESCRIPTION--